GENTOFTE KOMMUNES INFORMATIONSSIKKERHEDSPOLITIK

INDHOLDSFORTEGNELSE

1. INDLEDNING

Gentofte Kommunes Kommunalbestyrelse fastlægger med denne politik kravene til informationssikkerhed i Gentofte Kommune. Politikken omfatter såvel it-tekniske som manuelle behandlinger af informationer, herunder informationer lagret på elektroniske medier, papir, bånd mv.

Politikken har sit afsæt i ISO 27001, som er den generelle standard for styring af informationssikkerhed i den offentlige sektor, og i gældende lovgivning, herunder særligt EU databeskyttelsesforordningen, som træder i kraft 25. maj 2018.

1.1. Formål og målsætning

Informationssikkerhedspolitikken balancerer hensynet til driftssikkerhed på den ene side og muligheden for fortsat at udnytte digitaliseringsmulighederne til gavn for borgerne på den anden side. Lovgivningen stiller desuden en række specifikke krav til beskyttelse af personoplysninger og borgernes mulighed for at få indsigt i, hvad egne data anvendes til. Det betyder blandt andet, at kommunen skal beskrive uddybende bestemmelser for informationssikkerhed.

Politikken beskriver principperne for styring af informationssikkerhed i kommunen og, på overordnet niveau, de fysiske, tekniske og administrative processer, der beskytter fortrolighed, integritet og tilgængelighed af informationer. For en række processer og aktiver udarbejdes underliggende retningslinjer, som beskriver håndtering af konkrete risici.

1.2. Gyldighedsområde

Politikken er gældende for hele kommunen. Alle informationer og informationsaktiver (systemer, netværk, it-udstyr mv.), som er i kommunens varetægt og som anvendes i kommunen, er omfattet.

1.3. Godkendelse

Politikken er en del af kommunens styringsgrundlag og godkendes af kommunalbestyrelsen.

1.4. Gentofte Kommunes informationssikkerhedspakke

Gentofte Kommune arbejder med informationssikkerhed på flere niveauer, som illustreret ved nedenstående oversigt:

<table>
<tr><td colspan="4">Informationssikkerhedspolitik</td></tr>
<tr><td colspan="4">Operationelle bestemmelser</td></tr>
<tr><td>Retningslinjer for ledere</td><td>Retningslinjer for it-drift og digitalisering</td><td>Retningslinjer for it-brugere</td><td>Retningslinjer for eksterne parter</td></tr>
<tr><td colspan="4">Fælles processer og (kontrol)foranstaltninger</td></tr>
<tr><td colspan="4">Afdelingsspecifikke processer og (kontrol)foranstaltninger</td></tr>
</table>

Informationssikkerhedspolitik (dette dokument) beskriver rammer, mål, processer og overordnet organisering af informationssikkerhedsindsatsen og godkendes i Kommunalbestyrelsen.

Operationelle bestemmelser beskriver hvordan indholdet af informationssikkerhedspolitikken organiseres og konkretiseres bl.a. i forhold til drift, ansvar og roller. Disse godkendes af direktionen.

Retningslinjer beskriver, hvordan indholdet i Operationelle bestemmelser konkretiseres, og føres ud i organisationen. Der arbejdes med 4 retningslinjer, som i beskrivelserne vil stille krav til risikohåndtering på udvalgte områder.
Retningslinjerne skal være dækkende (bl.a. roller og ansvar) for de områder, de beskriver. Retningslinjer godkendes af 'Faggruppe for informationssikkerhed' (består af IT-Sikkerhedschefen som formand samt repræsentanter for organisationens fagområder) med inddragelse af forvaltninger og interessenter.

Fælles processer og (kontrol)foranstaltninger omfatter de centraliserede processer, herunder indkøb, projektstyring, rekruttering og it-drift. Her udarbejdes som hovedregel ikke særskilte sikkerhedsbeskrivelser af processer, men hvor der findes beskrivelser af processer og foranstaltninger, indarbejdes sikkerhedskravene. Deciderede sikkerhedsprocesser og sikkerhedsforanstaltninger samt kontrolforanstaltninger dokumenteres.

Afdelingsspecifikke processer og (kontrol)foranstaltninger omfatter de processer, der ikke kan centraliseres på grund af særlige forhold eller behov. Fx skoleelevers anvendelse af skolens it og eget it-udstyr på skolen.

2. POLITIK

2.1. Generelle krav

Der skal etableres en systematisk styring og koordinering af sikkerhed og for håndtering af risici og trusler, som opfylder følgende krav:

- Kontinuerlig identifikation af risici, trusler og sårbarheder
- Kontinuerlig vurdering af sikkerhedshændelser, alarmer og identificerede risici, trusler og sårbarheder i forhold til deres betydning for borgerne, opgavevaretagelsen og overholdelse af lovkrav.
- Identifikation og implementering af foranstaltninger, som minimerer sandsynlighed og konsekvens ved sikkerhedsbrud, og som eliminerer uacceptable risici.

2.2. Styring af sikkerhedskrav

2.2.1. Risikovurdering

Der skal foretages en fuld risikovurdering, som identificerer trusler og sårbarheder. Der skal foretages opfølgende risikovurderinger med passende mellemrum, der sikrer, at kommunens risikovurdering ifm. behandling af persondata er ajourført.

De nærmere krav hertil fastsættes i de Operationelle bestemmelser, der godkendes af direktionen.

2.2.2. Klassifikation

Data skal klassificeres efter konsekvenser ved brud på fortrolighed, integritet og tilgængelighed og beskyttelsen skal tilpasses efter klassifikationsniveau.

Informationsservices, herunder it-services, it-systemer, print, men også funktioner som fx postomdeling, skal klassificeres efter konsekvenser ved brud på fortrolighed, integritet og tilgængelighed og servicen skal tilpasses efter klassifikationsniveau.

Leverandører skal klassificeres efter, hvor kritiske de er i forhold til fortrolighed, integritet og tilgængelighed og deres mulighed for at påvirke informationssikkerheden i kommunen.

2.2.3. Overvågning af informationsservices

Kritiske informationsservices (systemer, netværk, opbevaring af data, arkiver mv.) skal kontinuerligt overvåges. Overvågningen skal beskyttes mod manipulation og utilsigtede afbrydelser.

2.2.4. Audits

Der skal foretages regelmæssige audits til sikring af, at kritiske services og foranstaltninger virker som forudsat. Hyppigheden af audits skal tilpasses risikoen. Audits skal dokumenteres.

De nærmere krav til audits og fastlæggelse af, hvem der udfører denne, skal fastsættes i de Operationelle bestemmelser, der godkendes af direktionen.

2.3. Roller og ansvar

Den enkelte medarbejders ansvar og afdelingernes ansvar skal være præcist og entydigt beskrevet med udgangspunkt i nedenstående overordnede organisering:

- Alle **medarbejdere** har pligt til at sætte sig ind i Gentofte Kommunes informationssikkerhedspolitik og efterleve de til enhver tid gældende retningslinjer. Det udarbejdes særskilte retningslinjer herfor: 'Retningslinjer for it-brugere'.

- Alle **personaleledere** har ansvar for, at kravene til system- og datasikkerhed i lederens ansvarsområde er klart kommunikeret til medarbejderne og at medarbejderne overholder kravene, ligesom lederen selv skal være bekendt med og overholde kravene til informationssikkerhed. Der udarbejdes særskilte retningslinjer herfor: 'Retningslinjer for ledere'.

- **Chefen for IT** er ansvarlig for, at it-driften lever op til informations-sikkerhedspolitikken og til aftaler med opgaveområderne. Undtaget er de aftaler, hvor der ikke er indgået en driftsaftale med IT.

- **JURA** - Kommunens juridiske kontor rådgiver organisationen om persondataretlige spørgsmål.

- **Databeskyttelsesrådgiveren (DPO)** varetager de opgaver, der påhviler denne iht. EU-databeskyttelsesforordningens artikel 39.

- **IT-sikkerhedschefen** har ansvar for udvikling, implementering og vedligeholdelse af kommunens informationssikkerhedsprogram og koordinerer aktiviteterne i årsplanen.

- **Sekretariatschefer** har inden for sekretariatets område ansvar for personaleledernes implementering og opfølgning på efterlevelse af politikken.

- **'Faggruppe for informationssikkerhed'** (består af IT-Sikkerhedschefen som formand samt repræsentanter for organisationens fagområder) fører tilsyn med efterlevelsen af politikken, behandler sager af principiel karakter og leverer en årlig statusrapport til direktionen.

- **Direktionen** - har det overordnede ansvar for informationssikkerheden og er ansvarlig for organisationens arbejde med informationssikkerhed på strategisk niveau, således at informationssikkerhedsmæssige overvejelser inddrages i alle væsentlige beslutninger.

- **Kommunaldirektøren** er øverste informationssikkerhedsansvarlige og godkender i samråd med direktionen de Operationelle bestemmelser.

- **Kommunalbestyrelsen** godkender informationssikkerhedspolitikken. De enkelte kommunalbestyrelsesmedlemmer er ligesom kommunens medarbejdere forpligtet til at følge kommunens informations-sikkerhedspolitik ifm. deres virke som kommunalbestyrelsesmedlemmer.

- **Ekstern IT-Revision** - Kommunens håndtering af IT-området er underlagt en ekstern IT-revision, der årligt gennemgår de forskellige områder og udfærdiger en IT-Revisionsrapport, der behandles i Direktionen.

For alle systemer udpeges på ledelsesniveau, en **systemejer** med ansvar for sikkerheden omkring systemet.

For alle persondatabehandlinger udpeges på ledelsesniveau, en **dataansvarlig**, som har ansvaret for at sikre at behandlingen er lovmedholdelig.

2.4. Sikkerhedskultur og -bevidsthed

Den enkelte medarbejder skal forholde sig til informationssikkerhed uanset niveau og opgave, og føle medansvar for, at der træffes de nødvendige forholdsregler. Både ledere og medarbejdere skal være opdaterede i forhold til de risici, som de kan påvirke i deres rolle og opgaver. Ledere på alle niveauer skal have et overblik over risikoen i deres område og har ansvaret for den løbende dialog med medarbejdere om risici og nødvendige forholdsregler for at håndtere dem.

2.4.1. Awareness

Der skal etableres et awareness-program, som udbreder kendskabet kommunens informationssikkerhedspolitik og de retlige krav i databeskyttelsesforordningen og databeskyttelsesloven. Programmet skal beskrive, hvordan de enkelte personalegrupper gøres bekendt med relevante risici. Effekten af de gennemførte awareness-aktiviteter skal måles og indgår i den løbende udvikling af programmet.

Der fastsættes nærmere krav i de Operationelle bestemmelser.

2.5. Sikker it-drift

Der skal opretholdes et driftsmæssigt stabilt, sikkert, let tilgængeligt og funktionelt it-serviceniveau. Opgaveområderne skal kunne stole på, at it-services, der etableres og leveres af It-afdelingen, er tilgængelige og beskyttet efter opgaveområdernes behov.

Sikkerhedsniveauet omkring it-services, som anvendes i kommunen, skal tydeligt deklareres og godkendes af ledelsen.

2.6. Adgang og rettigheder til data og systemer

Følsomme og kritiske systemer og data skal beskyttes mod uautoriseret adgang og ændring uanset, hvor de befinder sig. Adgang til og ændring af følsomme eller kritiske systemer eller data skal let kunne spores til personen.

De ansvarlige ledere skal gives let adgang til oplysninger, der er nødvendige for at kunne udføre ledelsestilsyn. Hvis der gives adgang til fortrolige data uden for det etablerede sikkerhedsmiljø, kræves en forudgående direktionsgodkendelse. Adgangskontrollens effektivitet skal efterprøves løbende for væsentlige og følsomme data og systemer.

Adgange til data skal minimeres og skal afspejle et aktuelt arbejdsbetinget behov. Kun en leder (eller en lederbemyndiget) kan anmode om ændrede rettigheder til sin medarbejder.

Der skal foretages stikprøver af anvendelse af adgange til personoplysninger. Omfanget af stikprøver skal tilpasses bredden af rettighederne og resultatet af tidligere stikprøver.

2.7. Projekter og indkøb

Digitaliseringsprojekter, herunder anskaffelse, udvikling og vedligeholdelse af it-systemer skal udformes, så de sikrer det fornødne sikkerhedsniveau og forbedrer og forenkler kommunens opfyldelse af lovgivningens krav til sikring af "de registreredes rettigheder".

Projekter og ændringer skal følge en fast, dokumenteret projekt- og/eller ændringsstyrings-proces. Sikkerhedsmæssig vurdering skal være en integreret del af projekt- og program-styringen, samt af udbudsprocessen.

Projekter, der har relation til behandling af personoplysninger, skal følge principperne for Databeskyttelse gennem design og standardindstillinger.

2.8. Fysisk beskyttelse af data og systemer

De fysiske omgivelser for informationer og informationsudstyr, der anvendes af kommunen og som kommunen har ansvaret for, beskytter effektivt mod fysiske hændelser, eksempelvis brand, vandskade, tyveri, hærværk, skader forårsaget af menneskelige fejl mv.

På steder, hvor der opbevares og anvendes informationer, systemer, infrastruktur og data, skal der etableres et risikotilpasset niveau af fysisk sikkerhed. Placering og den fysiske sikring af udstyr, som It-afdelingen har driftsansvaret for, skal forhåndsgodkendes af It-afdelingen. Den fysiske sikkerhed på lokationer med vitale installationer og informationer, der kræver høj beskyttelse, skal løbende efterprøves.

2.9. Eksterne parter

Det skal sikres, at samarbejdet med eksterne parter ikke kompromitterer Gentofte Kommunes målsætning for informationssikkerhed. Kravene til eksterne parter skal fastlægges ud fra politikken og ud fra en risikovurdering af det konkrete samarbejde. Eksterne parter skal dokumentere efterlevelsen af kravene og der skal ske løbende opfølgning. Der udarbejdes særskilte retningslinjer herfor: 'Retningslinjer for eksterne parter'.

2.10. Håndtering af sikkerhedshændelser

Der skal opretholdes et beredskab, så sikkerhedshændelser kan håndteres effektivt. Ved alvorlige hændelser skal der foretages en efterfølgende evaluering af hændelsen.

Sikkerhedsniveauet omkring de enkelte systemer og data fastlægges på baggrund af en risikovurdering og under hensyn til lovbestemte og kontraktlige krav.

2.11. Evaluering

IT-Sikkerhedschefen leverer en årlig status og forslag til ny årsplan, herunder omfanget af evaluering og opfølgning, til behandling i direktionen. Direktionen skal orienteres om alvorlige informationssikkerhedsbrud. Ved væsentlige personalerelaterede brud på sikkerheden involveres HR-chefen, som herefter behandler sagen.

3. IKRAFTTRÆDELSE OG ÆNDRINGER

Redigering af Informationssikkerhedspakken foretages af IT-Sikkerhedschefen og godkendes på følgende måde:

1. Forslag til ændringer til denne *Informationssikkerhedspolitik* udformes i samarbejde med JURA og databeskyttelsesrådgiveren til godkendelse af Kommunalbestyrelsen.
2. Ændringer i den *'De Operationelle bestemmelser'* udarbejdes med inddragelse af databeskyttelsesrådgiveren og godkendes af direktionen.
3. Informationssikkerhedspolitikkernes forskellige *'Retningslinjer'* udarbejdes og ændres i samarbejde med berørte afdelinger, med inddragelse af databeskyttelsesrådgiveren og godkendes af ledelsen i 'Borgerservice, Digitalisering og IT'.
4. Øvrige bilag omkring informationssikkerhedspolitikken er forankret i 'Faggruppe for Informationssikkerhed', som forestår udarbejdelse og ændringer i samarbejde med berørte afdelinger. Ændringer forelægges ledelsen i 'Borgerservice, Digitalisering og IT' én gang årligt.

Denne Informationssikkerhedspolitik er godkendt i Kommunalbestyrelse den 30. april 2018.